IFW

Attorney Docket No. 1032326-000025

2135

$ cc

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of

Gilles Lisimaque

Application No.: 09/576,412

Filed: May 22, 2000

For: PROCESS TO MANAGE DATA IN A CHIP CARD

Group Art Unit: 2135

Examiner: Beemnet Dada

Confirmation No.: 1838

SUBMISSION OF CERTIFIED COPY OF PRIORITY DOCUMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The benefit of the filing date of the following priority foreign application in the following foreign country under 35 U.S.C. § 119 is claimed in the Declaration.

Country:	France
Patent Application No.:	97 14802
Filed:	25 November 1997

In support of this claim, enclosed is a certified copy of said foreign application. Said prior foreign application is referred to in the oath or declaration and/or the Application Data Sheet. Acknowledgement of receipt of this certified copy is requested.

Charge the amount of $130.00 for the fee set forth in 37 C.F.R. §1.17(i) to our credit card. Form PTO-2038 is attached.

Respectfully submitted,

BUCHANAN INGERSOLL PC

Date: May 12, 2006

By: _____
James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

05/15/2006 SZEWDIE1 00000143 09576412
01 FC:1464 130.00 OP

R E P U B L I Q U E F R A N Ç A I S E

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 20 MARS 2006

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint-Petersbourg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr

DB 267/220104
ETABLISSEMENT PUBLIC NATIONAL CREE PAR LA LOI N° 51-444 DU 19 AVRIL 1951

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

Code de la propriété intellectuelle-Livre VI

N° 55-132

REQUÊTE EN DÉLIVRANCE

Confirmation d'un dépôt par télécopie ☐

Cet imprimé est à remplir à l'encre noire en lettres capitales

Réservé à l'INPI

DATE DE REMISE DES PIÈCES 25.11.97

N° D'ENREGISTREMENT NATIONAL 97 14802

DÉPARTEMENT DE DÉPÔT 75

DATE DE DÉPÔT 25 NOV. 1997

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

CABINET BALLOT SCHMIT
7, rue Le Sueur
75116 PARIS
FRANCE

n°du pouvoir permanent | références du correspondant | téléphone
CL/013754 | 01.40.67.11.99

2 DEMANDE Nature du titre de propriété industrielle

☒ brevet d'invention ☐ demande divisionnaire ☐ certificat d'utilité ☐ transformation d'une demande de brevet européen

demande initiale ☐ brevet d'invention ☐ certificat d'utilité n° date

Établissement du rapport de recherche ☐ différé ☒ immédiat

Le demandeur, personne physique, requiert le paiement échelonné de la redevance ☐ oui ☐ non

Titre de l'invention (200 caractères maximum)

PROCEDE DE GESTION DES DONNEES DANS UNE CARTE A PUCE

3 DEMANDEUR (S) n° SIREN 3 4 9 7 1 1 2 0 0 code APE-NAF

Nom et prénoms (souligner le nom patronymique) ou dénomination

GEMPLUS

Forme juridique
Société en Commandite par Action dite

Nationalité (s) française

Adresse (s) complète (s) Pays

Avenue du Pic de Bertagne
Parc d'activités de la Plaine de Jouques
13420 GEMENOS France

En cas d'insuffisance de place, poursuivre sur papier libre ☐

4 INVENTEUR (S) Les inventeurs sont les demandeurs ☐ oui ☒ non Si la réponse est non, fournir une désignation séparée

5 RÉDUCTION DU TAUX DES REDEVANCES ☐ requise pour la 1ère fois ☐ requise antérieurement au dépôt ; joindre copie de la décision d'admission

6 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE

pays d'origine	numéro	date de dépôt	nature de la demande

7 DIVISIONS antérieures à la présente demande n° date n° date

8 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE
(nom et qualité du signataire - n° d'inscription)

BALLOT Paul
92-1009
CABINET BALLOT SCHMIT

SIGNATURE DU PRÉPOSÉ À LA RÉCEPTION | SIGNATURE APRÈS ENREGISTREMENT DE LA DEMANDE À L'INPI

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION, CERTIFICAT D'UTILITE

DÉSIGNATION DE L'INVENTEUR
(si le demandeur n'est pas l'inventeur ou l'unique inventeur)

DIVISION ADMINISTRATIVE DES BREVETS

26bis, rue de Saint-Pétersbourg
75800 Paris Cédex 08
Tél. : 01 53 04 53 04 - Télécopie : 01 42 93 59 30 CL/013754

N° D'ENREGISTREMENT NATIONAL

9714802

TITRE DE L'INVENTION :

PROCEDE DE GESTION DES DONNEES DANS UNE CARTE A PUCE

LE(S) SOUSSIGNÉ(S)

BALLOT Paul
Cabinet BALLOT SCHMIT
7 rue Le Sueur
75116 PARIS
FRANCE

DÉSIGNE(NT) EN TANT QU'INVENTEUR(S) (indiquer nom, prénoms, adresse et souligner le nom patronymique) :

LISIMAQUE Gilles

domicilié au :

Cabinet BALLOT SCHMIT
7 rue Le Sueur
75116 PARIS
FRANCE

NOTA : A titre exceptionnel, le nom de l'inventeur peut être suivi de celui de la société à laquelle il appartient (société d'appartenance) lorsque celle-ci est différente de la société déposante ou titulaire.

Date et signature (s) du (des) demandeur (s) ou du mandataire

Paris, le 25 Novembre 1997

BALLOT Paul
92-1009
Cabinet BALLOT SCHMIT

BA 113/271195

PROCEDE DE GESTION DES DONNEES DANS UNE CARTE A PUCE

La présente invention a pour objet un procédé de gestion de données mémorisées dans une mémoire d'une carte à puce. L'invention concerne le transfert des informations d'une carte à une autre, notamment dans le cas où la carte de départ est sur le point d'être périmée et nécessite d'être remplacée par une carte à durée prorogée et possédant par ailleurs des mêmes facultés de système, des mêmes informations enregistrées dans le circuit électronique.

On connaît ainsi par exemple dans le domaine des cartes à pucs, ou plus généralement des objets portables à puce électronique, les porte-monnaies électroniques. Dans de telles utilisations, des unités monétaires stockées dans la mémoire d'une carte à puce sont transférées dans une autre et sont retirées de la première. Il n'y a pas, a priori, de limite de validité. On connaît par ailleurs dans le domaine bancaire des cartes à puce dont le corps de carte comporte un embossage indiquant en clair la date limite de validité de la carte. Cette précaution de limite de validité a deux intérêts. D'une part, elle permet de tenir compte du vieillissement des circuits électroniques et d'en favoriser le remplacement. D'autre part, elle provoque le retour à l'autorité de tutelle des cartes mises en circulation de façon à ce que cette autorité puisse globalement contrôler les moyens de transactions qu'elle met à disposition.

Avec le développement exponentiel des applications contrôlées par des utilisations de carte à puce, le remplacement des carte à puce périmées ne pourra plus nécessairement être effectué par une autorité de

tutelle: il devra pouvoir être effectué sur site, au besoin avec des lecteurs enregistreurs de cartes à puce communs.

Les principes d'utilisation des cartes à puce comportent la nécessité de composer un code secret, ou code personnel d'identification (PIN), et la comparaison de ce code à un code mémorisé dans la mémoire de la puce. En cas de succès de la comparaison, l'application, c'est-à-dire en pratique la délivrance d'un bien ou d'un service correspondant à la transaction, ou même un paiement, peut être effectuée avec la carte. Dans le cas contraire, le porteur est renvoyé à une situation de rejet. Cette comparaison est mise en oeuvre d'une manière sécurisée.

Le problème qui se pose lorsqu'on veut transférer des informations d'une carte dans une autre est un problème de gestion de ces codes secrets ou, plus généralement, des codes de gestion qui permettent la gestion sous contrôle des données mémorisées dans la mémoire des cartes. En effet, ces codes, mémorisés sous une forme ou sous une autre dans la mémoire de la puce de la carte, sont produits par l'autorité de tutelle en fonction de données propres à une identification de la carte et propres à cette autorité. De ce fait, il devient impossible d'organiser une prorogation automatique de la validité des cartes par remplacement des cartes périmées par des cartes à durées plus longues sans l'intervention de cette autorité. En effet, une telle démarche reviendrait à mettre à la disposition de tous les organismes, ou même de tous les lecteurs aptes à assurer cette prorogation, tous les secrets concernant l'élaboration des codes secrets et propres à cette autorité.

L'invention a néanmoins pour objet de remédier à ce

problème futur en instituant un protocole d'enregistrement des codes de gestion. Le protocole tient compte des anciens codes de gestion, ou au minimum d'informations relatives aux anciennes cartes dont proviennent les données qu'on va enregistrer dans la nouvelle.

Selon l'invention, on utilise un algorithme de cryptage, pour produire un nouveau code de gestion, qui prend en compte, d'une part, une information d'identification de la nouvelle carte et, d'autre part, une information relative à l'ancienne carte. Dans un cas particulier les informations relatives à l'ancienne carte seront les informations d'identification de l'ancienne carte. Dans un autre cas, ce sera le code de gestion de l'ancienne carte lui-même qui sera utilisé. Toute autre information relative à l'ancienne carte est utilisable.

Au moment de l'utilisation, on peut alors demander à l'utilisateur de composer un code secret qui correspond au code de gestion de la deuxième carte. Dans certains cas de vérification particulière, on pourra lui demander de composer en plus, en une deuxième étape ou une première étape, un code secret correspondant au code de gestion de la première carte afin de vérifier la cohérence de l'élaboration du deuxième code de gestion.

L'invention a donc pour objet un procédé de gestion de données mémorisées dans une première mémoire d'une première puce d'une première carte à puce dans lequel

- on produit un premier code de gestion, avec un premier algorithme de cryptage, à partir d'une clé mère et d'une première information d'identification de la première carte à puce,

- on enregistre ce premier code de gestion dans la

première mémoire,

- on met la première carte en relation avec un lecteur de carte à puce,

- on autorise une édition de données mémorisées dans la première mémoire si un code présenté dans le lecteur est compatible avec le premier code de gestion enregistré,

caractérisé en ce que

- on produit un deuxième code de gestion, avec un deuxième algorithme de cryptage, à partir d'une information relative à la première carte et d'une deuxième information d'identification d'une deuxième carte à puce,

- on enregistre cette information relative à la première carte et ce deuxième code de gestion dans une deuxième mémoire d'une deuxième puce de la deuxième carte à puce

- on autorise l'édition de données mémorisées dans la deuxième mémoire si un code secret présenté par le lecteur est compatible avec le deuxième code de gestion enregistré.

L'invention sera mieux comprise à la lecture de la description qui suit et à l'examen des figures qui l'accompagnent. Celles-ci ne sont données qu'à titre indicatif et nullement limitatif de l'invention. Les figures montrent:

- Figure 1: Une représentation schématique d'un dispositif utilisable pour mettre en oeuvre le procédé de l'invention;

- Figure 2: Les étapes essentielles de la mise en oeuvre du procédé de l'invention;

- Figure 3: Le mode préféré de vérification de la légalité de la détention d'une carte à puce par un porteur;

- Figure 4: La représentation schématique d'un algorithme de type symétrique permettant de retrouver un code de gestion à partir d'un précédent code de gestion.

La figure 1 montre un dispositif utilisable pour mettre en oeuvre le procédé de gestion de données de l'invention. Cette figure montre un lecteur 1 pour lire un objet 2 portable à puce, ou une carte à puce, introduit dans une fente 3 du lecteur. Ce lecteur comporte d'une manière conventionnelle un écran 4 pour visualiser des messages édités par le lecteur et un clavier 5 pour permettre à un opérateur, le porteur de la carte, d'organiser une transaction entre le lecteur 1 et la carte à puce 2. Dans un exemple, le lecteur peut être relié par divers moyens à un système maître 6, soit en temps réel, soit en temps différé. Dans un exemple, ces moyens peuvent comporter une liaison hertzienne par l'intermédiaire de deux antennes 7 et 8, et leur système d'émission réception associé, reliés au lecteur et au système maître respectivement.

L'invention concerne plus particulièrement le transfert d'informations contenues dans un carte à puce 9 périmée (sa date de péremption étant par exemple 1996, déjà passée) et une carte à puce nouvelle 2 avec une date de validité bien supérieure (2007). La carte 9 ainsi que la carte 2 comportent chacune une puce électronique telle que référencée 10 et des moyens de mise en relation avec le lecteur 1. Dans un exemple, ces moyens de mise en relation sont tout simplement un connecteur 11. D'autres solutions de mise en relation sont connues.

Sur la figure 2, on a montré d'une manière plus détaillée les étapes du procédé de l'invention. On y a également représenté les carte à puce 9 ancienne et 2

nouvelle. La carte à puce est munie, enregistrée dans une mémoire de la puce, d'une information 12 représentative d'un numéro de série de la carte ou de la puce. Dans une application bancaire, ce numéro de série peut également être ou correspondre à un numéro de compte en banque.

Le principe de l'élaboration d'un code de gestion consiste à utiliser une clé mère 100. Une clé mère est ainsi une chaîne de caractères binaires: dans un exemple, une clé mère a une longueur de 1024 bits. Le numéro de série de la carte ou de la puce peut également être présenté sous une forme binaire. Les deux chaînes de caractères binaires correspondantes sont alors présentées à un algorithme de cryptage représenté symboliquement par la référence 13. L'algorithme 13 de cryptage a pour résultat la production d'un premier code de gestion. Dans un exemple, l'algorithme 13 de cryptage est mis en oeuvre par le système maître, disponible chez un émetteur de la carte, avant que cet émetteur ne décide d'envoyer la carte à puce à son utilisateur. Au cours d'une opération dite de personnalisation, l'émetteur, avec un lecteur de carte à puce spécial, lit le numéro de série de la carte et produit, avec un algorithme 13 et une clé mère 100 connue de l'émetteur seul, un premier code 14 de gestion. Le système maître enregistre le premier code 14 de gestion dans la mémoire de la puce de la carte. D'une manière connue, cet enregistrement peut être effectué à un emplacement de la puce de la carte 9. Cet emplacement peut aussi dépendre pour sa localisation de l'application, première application 27, gérable avec la carte. De préférence, les codes de gestion sont donc secrets et mémorisés dans des emplacements inviolables.

La figure 3 montre, un mode d'utilisation préféré d'une carte à puce ou d'un objet portable à puce muni pour une application d'un tel code de gestion 14. Au moment où un opérateur, un utilisateur, glisse sa carte à puce dans le lecteur 1, celui-ci produit, un aléa 15, un chaîne aléatoire de bits. Cet aléa 15 est envoyé, notamment par l'intermédiaire du connecteur 11, à la puce de la carte 9. Celle-ci met alors en oeuvre un cryptage de l'aléa 15 par le code de gestion 14 et produit un code 16 de gestion crypté par l'aléa. Dans le même temps, l'opérateur compose sur le clavier 5 un code secret. Ce code secret est envoyé au lecteur 1. Le lecteur 1 effectue, de la même façon que la carte 9, le cryptage 17 du code secret par la valeur de l'aléa 15 que ce lecteur connaît. Un circuit de comparaison 18 du lecteur, à moins que cela ne soit un circuit de comparaison 19 de la carte, effectue la comparaison du code 16 de gestion crypté par l'aléa au code secret 17 crypté par l'aléa. S'il y a identité le résultat du circuit de comparaison 18 ou 19 sera positif et la suite de la transaction envisagée avec la carte 9 pourra se poursuivre.

Notamment, cette suite de transactions comportera l'édition de données mémorisées dans la première mémoire de la première carte 9 si le code secret présenté au lecteur est compatible avec le premier code 14 de gestion enregistré.

En effet, le lecteur produira souvent, d'une part, un ticket 20 représentatif de la transaction ou, d'autre part, d'une manière non visible, un enregistrement dans sa mémoire représentatif de cette transaction. Cet enregistrement est lui-même destiné à être transmis au système maître en mode différé ou en temps réel. Le ticket 20 ainsi que l'enregistrement

comporteront des indications de la transaction, notamment au moins une partie d'identification de la carte à puce 2, par exemple le numéro de série 12 envisagé jusqu'ici, ou un numéro de compte ou toute autre information enregistrée dans la carte 9. Le seul fait que ces informations apparaissent sur le ticket 20, ou sur l'enregistrement du lecteur 1, signifie qu'elles ont par ailleurs été éditées. Dans la pratique, on cherche en fait avec la comparaison à bloquer ou à permettre une telle édition et donc la suite de la transaction.

Dans l'invention, on a considéré qu'on avait affaire à une carte 9 et qu'on voulait passer le contenu de la puce 10 de cette carte 9 dans une puce d'une nouvelle carte 2. Selon l'invention, on produit avec un algorithme 21, à partir d'une information relative à la carte 9 et d'une information d'identification de la deuxième carte 2 un deuxième code de gestion 22.

Dans un exemple particulier, l'information relative à la première carte est justement le numéro de série 12 et l'information relative à la deuxième carte 9 est également un numéro de série 23 de cette deuxième carte. Néanmoins, on aurait pu utiliser comme information relative à la première carte le premier code de gestion 14, ou toute autre information.

Dans l'invention, la mise en oeuvre de l'algorithme 21 est effectuée par un lecteur 1 de type commun, mais muni d'un logiciel pour, au cours d'une cession de production du code 22, provoquer la lecture dans la carte 9 des informations utiles, demander l'extraction de la carte 9 et la mise en place de la carte 2 en remplacement, lire les données d'identification utiles dans la carte 2, calculer le code 22 et l'enregistrer

dans la carte 2. Pour simplifier cette production des codes de gestion, le logiciel de mise en oeuvre de l'algorithme peut être, au moins en partie, mémorisé dans la carte 9 (ou et dans la carte 2). La mise en oeuvre peut même être effectuée par le micro-processeur de la carte pour plus de sécurité.

Pour simplifier l'explication on a considéré que l'algorithme 21 nécessitait la réception de trois chaînes de caractères. L'algorithme 13 recevra de préférence le premier numéro de série 12, une deuxième fois le premier numéro de série 12 ainsi que la clé mère 100. Dans un exemple, l'algorithme 21 est le même que l'algorithme 13. Pour l'algorithme 21 les trois informations utiles peuvent être le numéro de série 23, le numéro de série 12 et la clé mère 100. Cette clé 100 peut même être remplacée par le code 14. On produit donc bien selon l'invention un deuxième code de gestion 22 avec le deuxième algorithme de cryptage 21. Le deuxième code de gestion 22 ainsi produit est alors enregistré dans la deuxième carte 2 en même temps que l'information relative à la première carte (12 ou 14) qui a servi à l'élaboration de ce deuxième code de gestion. Dans l'exemple, le numéro de série 12 de la première carte 9 est également enregistré dans la deuxième carte 2.

La figure 2 montre encore que le mécanisme peut se prolonger à partir du moment où on utilisera une troisième carte à puce 24 munie d'un troisième numéro de série 25. On pourra alors, avec cette troisième carte 24, produire un troisième code de gestion 26 dans les mêmes conditions avec un algorithme 27 semblable à l'algorithme 21. Dans ce cas, on stockera dans la mémoire de la troisième carte 24 les informations relatives à la deuxième carte 2: le numéro de série 23.

Cependant, on peut vouloir également stocker dans la troisième carte 24 l'information relative à la première carte 9, c'est-à-dire le numéro de série 12.

On a représenté pour la carte 9 une première application 27. Cette application est une première façon d'utiliser la carte 9. Cette carte 9 peut être, de préférence selon l'invention, une carte multi-applications. Dans ce cas, le code de gestion 14 est un code de gestion destiné à une application. Pour des autres applications 28 ou 29, on retrouvera les mêmes éléments. Cependant, autant on peut utiliser un même numéro de série 12 (commun à toute la carte ou à toute la puce), autant les autres codes de gestion auront intérêt à être différents. Ceci peut être facilement obtenu en utilisant des algorithmes 13 paramétrés par des clés mères 100 différentes, dépendantes des applications concernées. La clé mère 100 peut par ailleurs être stockée dans la carte 9 à l'endroit de la zone mémoire dévolue à l'application 27, 28 ou 29. L'algorithme 13 est alors paramètré par une clé 100 qui dépend de l'application.

Au moment de la reconnaissance de ce que le porteur de la carte 2 est un bon porteur, le lecteur 1 et la carte à puce 2 échangent des informations conformément à la figure 2. Dans ce cas cependant, le code de gestion concerné est maintenant sera le code 22 relatif à la deuxième carte et non plus le code 14 relatif à la première. L'opérateur doit donc composer un code secret correspondant au code 22.

Il est possible selon l'invention de vérifier que la deuxième carte 2 est une héritière légitime du contenu de la première carte 9. Cette vérification peut être entreprise à la demande, en faisant exécuter par le lecteur 1, ou alternativement par la carte à puce 2,

des opérations de cryptage correspondant, d'une part, à l'algorithme 13 et, d'autre part, aux algorithmes 16 et 17. L'opérateur doit donc composer un code secret correspondant au code 22. Autrement dit, à partir du premier numéro de série 14 disponible dans la deuxième carte 2, il est possible, conformément aux indications données pour le haut de la figure 2, de retrouver le premier code de gestion 14. Puis, nanti de ce code de gestion 14, la carte 2 peut mettre en oeuvre l'algorithme 16 à partir de l'aléa. Dans ce cas, on peut demander au porteur de composer, non pas le nouveau code secret, mais l'ancien code secret. Dans un exemple la demande de réalisation de cette vérification plus complexe pourra être aléatoirement demandée, par exemple une fois sur cent en moyenne. Evidemment, en cas d'échec de la vérification les mêmes conséquences sur le déroulement de la suite de la transaction seront entraînées.

L'algorithme 21 sera de préférence différent de l'algorithme 13, encore qu'il pourrait être le même. S'il est différent, l'algorithme 21 sera de préférence un algorithme dit symétrique. Un algorithme symétrique 31 est montré sur la figure 4. La particularité d'un algorithme symétrique est d'utiliser des clés publiques CPu appariées à des clés privées CPr. Le caractère symétrique de l'algorithme 31 résulte ensuite dans le fait que des données 30 chiffrées dans l'algorithme 31 symétrique par la clé mère 32 produisent des données cryptées 33. Si ces données 33 sont elles-mêmes cryptées par le même algorithme 31 paramètré, ensuite par la clé fille 34, alors la deuxième mise en oeuvre de l'algorithme 31 produit les données 30 de départ. Dans un exemple, pour une même clé publique mère CPu on peut avoir beaucoup de clés privées filles CPr

différentes. La diversification des clés fait intervenir le numéro de série des cartes, de sorte que chaque carte possède une clé, un code de gestion 14 différent. On voit que, si l'algorithme 13 ou l'algorithme 21 sont des algorithmes symétriques, et si on remplace les données 30 par le numéro de série 12, alors on obtient à titre de données cryptées la clé fille 34 elle-même.

Selon l'invention, on associe en plus aux données mémorisées dans la mémoire de la carte 9 un attribut de transmission. Et on autorise l'édition de ces données, notamment en vue de leur copie dans la deuxième mémoire, en fonction de la valeur de cet attribut. Lorsque c'est le cas, on copie ces données dans la deuxième carte à puce 2 en même temps que cet attribut. En pratique, cet attribut renseigne sur une nécessité de produire un deuxième code de gestion ou non au moment de la copie. Dans certains cas, le mécanisme mis en oeuvre par les algorithme 13 et 21 sera rendu nécessaire, dans d'autres cas il ne sera pas exécuté.

Dans un autre cas, l'attribut de transmission renseigne sur la nécessité du contrôle de la copie par le système maître. Dans ce cas, au moment où on édite les données à copier, on lit l'attribut qui les concerne. Si l'intervention du système maître est requise une connexion au système maître 6 est entreprise. Cette copie peut avoir lieu ensuite en temps réel ou en temps différé avec ou non transmission des données au système maître.

REVENDICATIONS

1 - Procédé de gestion de données mémorisées dans une première mémoire d'une première puce (10) d'une première carte (9) à puce dans lequel

- on produit (13) un premier code (14) de gestion, avec un premier (13) algorithme de cryptage, à partir d'une clé mère (100) et d'une première information (12) d'identification de la première carte à puce,

- on enregistre ce premier code de gestion dans la première mémoire,

- on met la première carte en relation avec un lecteur (1) de carte à puce,

- on autorise une édition (20) de données mémorisées dans la première mémoire si un code secret présenté dans le lecteur est compatible (18,19) avec le premier code de gestion enregistré,

caractérisé en ce que

- on produit (21) un deuxième code (22) de gestion, avec un deuxième algorithme (21) de cryptage, à partir d'une information (12) relative à la première carte et d'une deuxième (23) information d'identification d'une deuxième carte à puce,

- on enregistre cette information (12) relative à la première carte et ce deuxième code (22) de gestion dans une deuxième mémoire d'une deuxième puce de la deuxième carte (2) à puce

- on autorise l'édition de données mémorisées dans la deuxième mémoire si un code secret présenté dans le lecteur est compatible avec le deuxième code de gestion enregistré.

2 - Procédé selon la revendication 1, caractérisé en ce que

- les premiers et deuxièmes codes de gestion sont des codes secrets.

3 - Procédé selon l'une des revendications 1 ou 2, caractérisé en ce que

- le deuxième algorithme est mis en oeuvre dans la puce de la carte.

4 - Procédé selon l'une des revendications 1 à 3, caractérisé en ce que

- le premier algorithme de cryptage est différent du deuxième algorithme de cryptage, et en ce que

- le deuxième algorithme de cryptage est symétrique (31).

5 - Procédé selon l'une des revendications 1 à 3, caractérisé en ce que

- le premier algorithme de cryptage est le même que le deuxième algorithme de cryptage.

6 - Procédé selon l'une des revendications 1 à 5, caractérisé en ce que

- l'information relative à la première carte est la première information d'identification de la première carte ou de la première puce.

7 - Procédé selon l'une des revendications 1 à 6, caractérisé en ce que

- l'information relative à la première carte est le premier code de gestion de la première carte ou de la première puce.

8 - Procédé selon l'une des revendications 1 à 7, caractérisé en ce que

- on produit, par exemple, dans le lecteur (1) un mot code de gestion sur la base de l'information

relative à la première carte et

- on vérifie que la carte est authentique si ce deuxième mot code de gestion est compatible avec un mot secret.

9 - Procédé selon l'une des revendications 1 à 8, caractérisé en ce que

- on associe aux données mémorisées dans la première mémoire un attribut de transmission,

- on autorise l'édition de ces données, en vue de leur copie dans la deuxième mémoire, en fonction de la valeur de cet attribut,

- on copie ces données et cet attribut dans la deuxième mémoire,

- cet attribut renseigne sur une nécessité de produire un deuxième code secret au moment de la copie.

10 - Procédé selon la revendication 9, caractérisé en ce que, pour n'autoriser l'édition des données contenues dans la première mémoire que sous le contrôle d'un système maître,

- on associe un attribut de transmission qui renseigne sur une nécessité de ce contrôle par un système maître,

- on lit cet attribut préalablement à l'édition,

- et on lance un programme d'édition si l'attribut lu le permet.

11 - Procédé selon l'une des revendications 9 à 10, caractérisé en ce que

- l'attribut de transmission interdit l'édition en vue de la copie des données concernées.

12 - Procédé selon l'une des revendications 9 à 11, caractérisé en ce que

- on copie en différé les informations dans la

deuxième mémoire.

13 - Procédé selon l'une des revendications 1 à 112, caractérisé en ce que

- la carte est une carte multi-applications (27-29), les données étant associées à des codes de gestion respectifs.

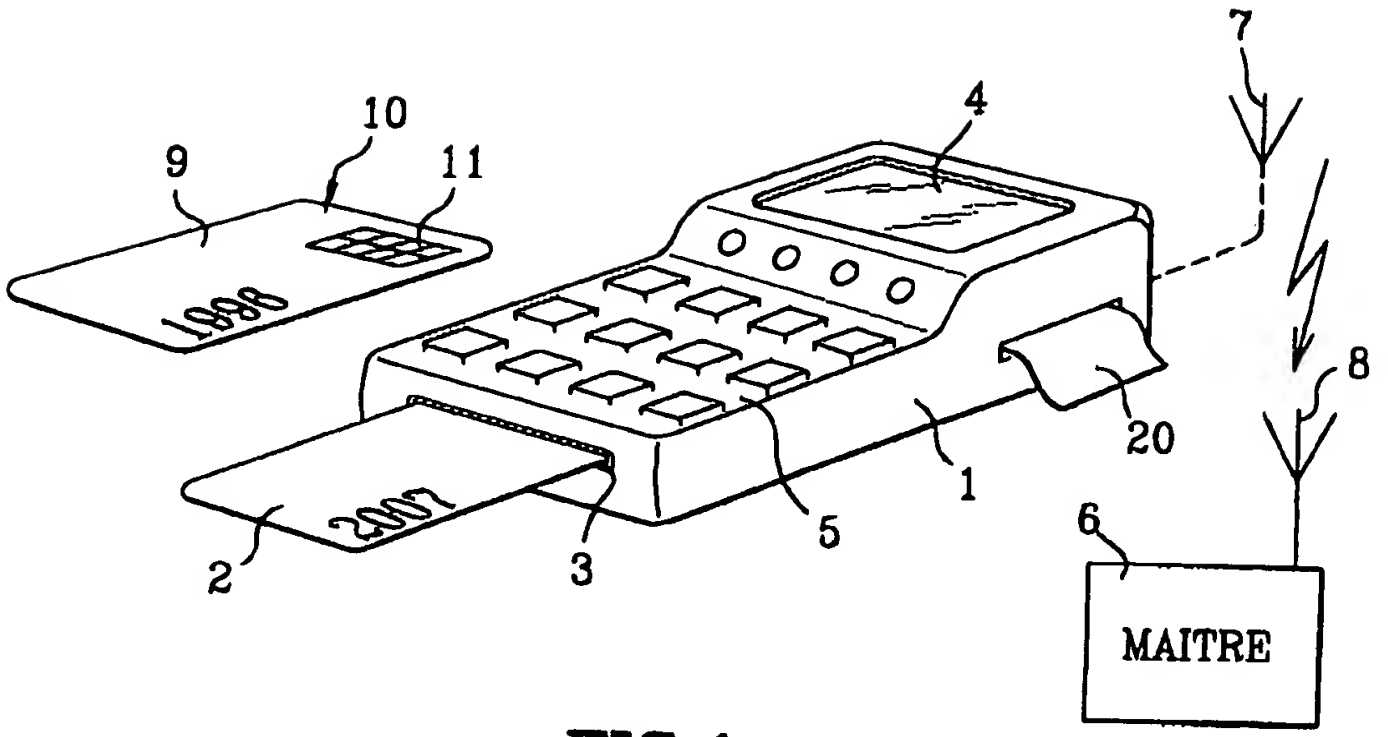
7
10
9
11
4
8
20
1
5
6
2
3
MAITRE

FIG.1

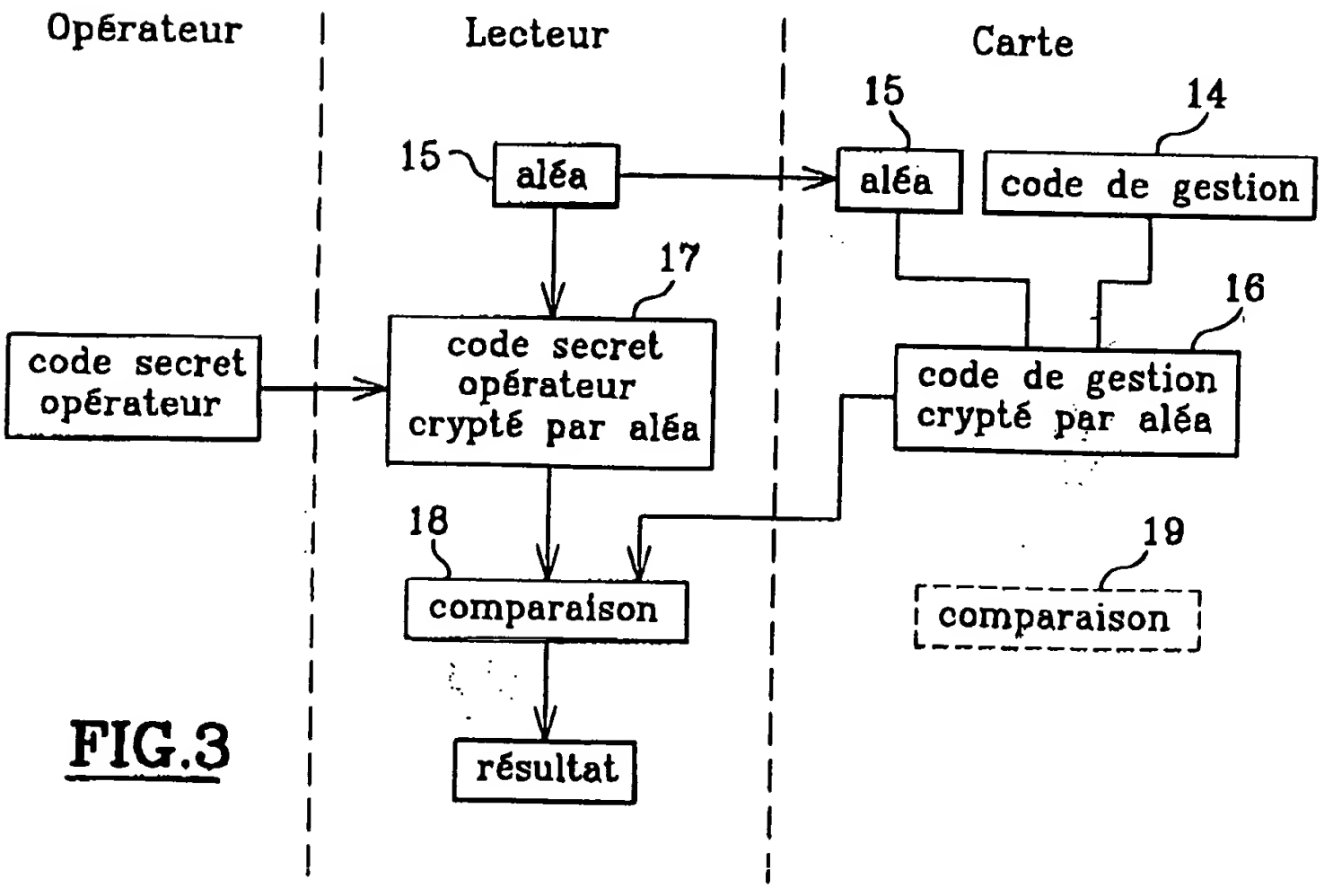
Opérateur
Lecteur
Carte
15
14
15
aléa
aléa
code de gestion
17
16
code secret opérateur
code secret opérateur crypté par aléa
code de gestion crypté par aléa
18
19
comparaison
comparaison
résultat

FIG.3

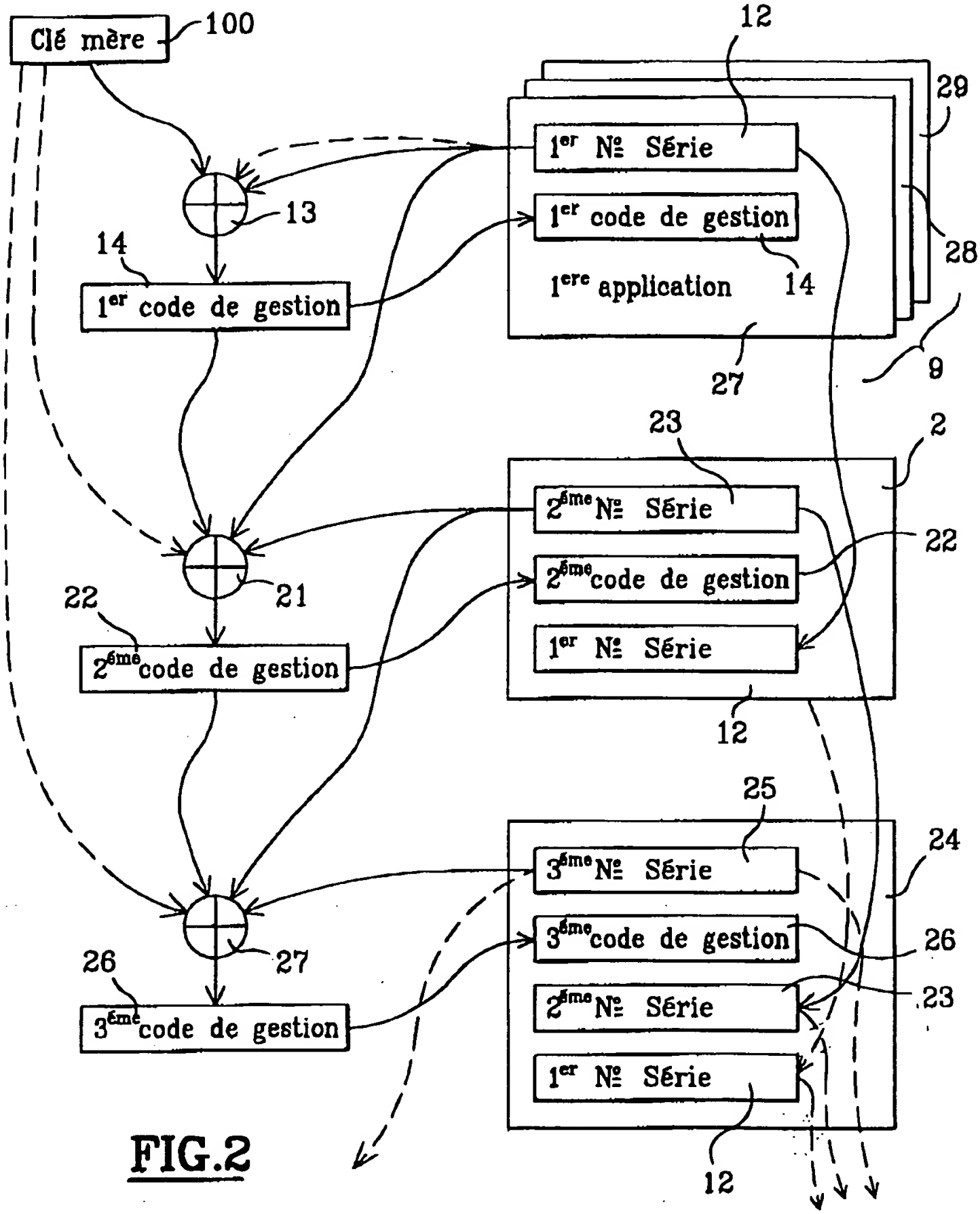
Clé mère
100
12
29
1er Nº Série
1er code de gestion
1ere application
14
28
13
14
1er code de gestion
9
27
23
2
2ème Nº Série
22
2ème code de gestion
1er Nº Série
21
22
2ème code de gestion
12
25
24
3ème Nº Série
3ème code de gestion
26
2ème Nº Série
23
1er Nº Série
27
26
3ème code de gestion
12

FIG.2

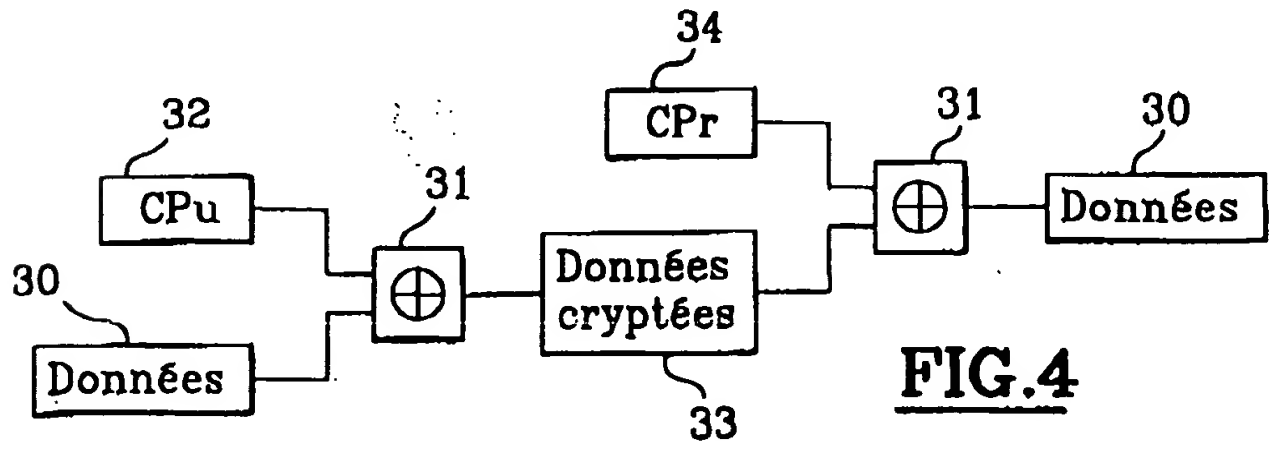
34
CPr
32
CPu
31
31
30
Données
30
Données
Données cryptées
33

FIG.4